Juice Jacking là gì? Vì sao không nên sạc điện thoại ở nơi công cộng?

Có một tình huống khá là phổ biến như sau. Giả sử chiếc điện thoại yêu quý của bạn đang dần cạn pin trong khi bạn lại đang có một cuộc trò chuyện thú vị với cô bạn gái mới quen trên Facebook, và "tin tốt" là bạn để quên cục sạc chết tiệt ở nhà, rồi bỗng nhiên bạn thấy một cột sạc USB công cộng ở góc đường. Không do dự, bạn cắm điện thoại của mình vào và tiếp tục tận hưởng những hương vị ngọt ngào từ cuộc trò chuyện đang dang dở kia. Cảm giác thoải mái đó có thể khiến bạn trở thành nạn nhân của các hacker, những kẻ muốn thu thập thông tin cá nhân của bạn và làm lợi từ những thông tin đó.

Jacking Juice chính xác là gì?

Bất kể loại điện thoại thông minh hiện đại nào ngày nay, có thể là các thiết bị Android, iPhone hoặc BlackBerry đều có một tính năng chung đó là nguồn điện sạc và luồng dữ liệu truyền qua trên cùng một cổng và một đường dây cáp. Cho dù bạn đang sử dụng kết nối USB miniB, USB typeC chuẩn hiện nay hay cáp Lightning độc quyền của Apple đi chăng nữa, thì cáp được sử dụng để sạc pin cũng kiêm luôn chức năng truyền và đồng bộ hóa dữ liệu trên điện thoại.

“Chỉ bằng việc cắm điện thoại vào một nguồn sạc không xác định, thiết bị của bạn có nguy cơ bị nhiễm mã độc. Bạn có thể phải trả giá bằng toàn bộ dữ liệu của mình”, chuyên gia bảo mật Drew Paik của Authentic8 giải thích.

Các điểm sạc điện thoại và Wi-Fi công cộng thường được tìm thấy ở những nơi như sân bay, máy bay, công viên hay các trung tâm hội nghị. Kết nối điện thoại tại các điểm sạc này mang đến những nguy cơ không hề nhỏ.

"Loại dây bạn dùng để sạc điện thoại cũng là dây dẫn dữ liệu từ điện thoại đến thiết bị khác. Chẳng hạn, khi bạn kết nối iPhone với máy Mac bằng dây sạc, bạn có thể tải ảnh từ điện thoại sang Mac. Nếu cổng sạc công cộng bị hack, kẻ xấu có thể truy cập không giới hạn đến các dữ liệu của bạn", ông Paik giải thích thêm.

Dữ liệu đó có thể là email, tin nhắn, ảnh hoặc địa chỉ liên hệ. Biện pháp hack thông tin này được gọi là “juice jacking” – thuật ngữ được sáng tạo ra từ năm 2011. Năm ngoái, người ta cũng phát hiện ra phương pháp “video jacking”, sử dụng các cổng kết nối bị hack và màn hình của điện thoại để ghi lại tất cả những gì người dùng gõ và nhìn vào.

Có thể hiểu đơn giản đây là những vụ xâm phạm vào quyền riêng tư. Cụ thể những dữ liệu như ảnh riêng tư và thông tin liên hệ sẽ được sao chép sang thiết bị độc hại thông qua các kết nối với thiết bị sạc công cộng. Ngoài ra các hacker cũng có thể truyền các mã độc trực tiếp vào thiết bị của bạn rồi sau đó sẽ lấy cắp thông tin trong một khoảng thời gian dài. Tại hội nghị an ninh BlackHat năm nay, các chuyên gia nghiên cứu bảo mật Billy Lau, YeongJin Jang và Chengyu Song đã trình bày về chủ đề “MACTANS: Đưa các phần mềm độc hại vào thiết bị iOS thông qua các bộ sạc không đảm bảo” và đây là trích đoạn từ bài thuyết trình của họ:

“Trong bài thuyết trình này, chúng tôi xin trình bày về cách thức các thiết bị iOS có thể bị xâm phạm chỉ trong vòng một phút sau khi chúng được cắm vào một bộ sạc độc hại. Trước tiên chúng ta sẽ cùng xem xét các cơ chế bảo mật hiện có của Apple để bảo vệ chống lại việc cài đặt phần mềm tùy ý, sau đó mô tả các khả năng mà cổng USB có thể được tận dụng làm công cụ để vượt qua các cơ chế bảo vệ này. Để chứng minh sự tồn tại của các mã độc, chúng tôi sẽ chỉ cho các bạn thấy kẻ tấn công có thể ẩn các phần mềm độc hại của chúng theo cách giống như cách Apple giấu các ứng dụng tích hợp của riêng họ. Để chứng minh những hậu quả

trong thực tế của các lỗ hổng bảo mật này, chúng tôi đã thu thập các thông tin về khái niệm bộ sạc độc hại sử dụng BeagleBoard, được gọi là Mactans".

Sử dụng phần cứng giá rẻ và lợi dụng lỗ hổng bảo mật trên thiết bị, các hacker có thể truy cập vào các thiết bị iOS hiện tại trong vòng chưa đến một phút, mặc dù có rất nhiều biện pháp bảo mật mà Apple đã đưa ra để ứng phó với vấn đề này.

Trong nhiều năm trước, tại hội nghị an ninh DEF CON 2011, các nhà nghiên cứu bảo mật từ Aires Security: Brian Markus, Joseph Mlodzianowski, và Robert Rowley, đã xây dựng một ki-ốt sạc để chứng minh cụ thể sự nguy hiểm của Juice Jacking và cảnh báo cho công chúng biết được những nguy hiểm khi kết nối điện thoại với các ki-ốt sạc độc hại.

Thậm chí rắc rối hơn là việc tiếp xúc với các ki-ốt sạc độc hại có thể tạo ra một vấn đề bảo mật kéo dài ngay cả khi thiết bị không còn kết nối với ki-ốt sạc đó nữa. Trong một bài viết gần đây về chủ đề này, nhà nghiên cứu bảo mật Jonathan Zdziarski nêu ra cách các lỗ hổng ghép nối trên iOS vẫn tồn tại và có thể cung cấp cho người dùng độc hại cửa sổ thiết bị của bạn ngay cả sau khi bạn không còn liên lạc với kiốt nữa:

"Nếu bạn không nắm rõ được cách thức ghép nối trên iPhone hoặc iPad, thì đây là cơ chế ghép nối mà máy tính của bạn thiết lập mối kết nối đáng tin cậy với điện thoại, qua đó có thể kết nối với iTunes, Xcode hoặc các công cụ khác. Khi một máy tính để bàn đã được ghép nối với điện thoại, nó có thể truy cập một loạt thông tin cá nhân trên điện thoại đó, bao gồm danh bạ, ghi chú, ảnh, bộ sưu tập nhạc, cơ sở dữ liệu sms, bộ nhớ đệm và thậm chí có thể sao lưu toàn bộ dữ liệu trên điện thoại. Khi một thiết bị được ghép nối, tất cả điều này và nhiều thứ khác có thể được truy cập không dây bất cứ lúc nào, bất kể bạn có bật đồng bộ hóa WiFi hay không. Có thể ví những phần mềm độc hại này như một loại virus mãn tính, chúng chỉ biến mất khi iPhone hoặc iPad của bạn khôi phục lại cài đặt bạn đầu".

Làm cách nào để tránh bị Juice Jacking?

Mặc dù Juice Jacking hiện không phải là mối đe dọa phổ biến như trộm cắp điện thoại hoặc tiếp xúc với vi-rút độc hại thông qua các dữ liệu tải xuống, bạn vẫn nên thực hiện các biện pháp phòng ngừa thông thường để tránh tiếp xúc với các hệ thống có thể truy cập độc hại vào thiết bị cá nhân của bạn.

Cách phòng ngừa hữu hiệu và đơn giản nhất đơn giản là hạn chế hoặc tránh hẳn việc sạc điện thoại từ các hệ thống sạc của bên thứ ba:

Giữ cho thiết bị của bạn không cạn pin: Hãy tạo thói quen sạc điện thoại tại nhà và văn phòng của bạn khi bạn không sử dụng đến chúng. Công nghệ pin hiện tại cho phép bạn sạc nhồi, cắm rút sạc thoải mái mà không lo chai pin, vậy nên hãy cố gắng giữ cho smartphone của bạn luôn đủ năng lượng trước khi bạn ra ngoài. Ngoài việc đảm bảo điện thoại của bạn được duy trì pin đầy đủ, bạn còn có thể sử dụng thêm các ứng dụng hỗ trợ quản lý năng lượng, hỗ trợ tiết kiệm pin. Hiệu quả của các ứng dụng này vẫn còn tương đối mơ hồ, nhưng chắc chắn vẫn tốt hơn là không làm gì cả.

Sử dụng sạc dự phòng: Đây là cách sạc pin điện thoại phổ biến và tiện lợi nhất hiện nay trong trường hợp bạn không ở nhà, đơn giản chỉ cần cắm điện thoại vào pin để sạc pin bất cứ khi nào bạn muốn. Sử dụng cách sạc này, bạn sẽ không phải lo về vấn đề bảo mật, nhưng đổi lại bạn sẽ tốn một khoản chi phí nhỏ để mua pin dự phòng cũng như chọn loại phù hợp để hạn chế những nguy cơ về cháy nổ khi chẳng may mua phải loại kém an toàn.

Sử dụng bộ sạc riêng của bạn với ổ cắm AC: Trong một số trường hợp, các trạm sạc công cộng có thể có cả ổ cắm điện AC tiêu chuẩn lẫn cổng sạc USB nhằm ứng nhu cầu về tốc độ sạc. Trong trường hợp này, hãy bỏ qua các cổng sạc USB mà cắm trực tiếp bộ sạc tiêu chuẩn của điện thoại vào ổ cắm điện AC. Sẽ không có bất cứ nguy cơ về bảo mật nào khi bạn sử dụng ổ cắm điện AC ngay cả khi lưu lượng mạng đang được truyền qua dây điện. Thiết bị của bạn sẽ được an toàn miễn là bạn sử dụng một bộ sạc đáng tin cậy.

Khóa điện thoại của bạn: Khi điện thoại của bạn bị khóa, nó sẽ không thể ghép nối được với thiết bị được kết nối. Đơn cử như các thiết bị iOS sẽ chỉ ghép nối khi được mở khóa. Nhưng một lần nữa, như chúng tôi đã nêu trước đó, việc ghép nối chỉ diễn ra trong vài giây, do đó bạn nên đảm bảo rằng điện thoại của mình đã thực sự bị khóa khi sạc.

Tắt nguồn điện thoại: Phương pháp này chỉ áp dụng đối với một số mẫu điện thoại nhất định. Mặc dù điện thoại bị tắt nguồn, nguồn trên toàn bộ mạch USB vẫn được bật và cho phép truy cập vào bộ nhớ flash trong thiết bị.

Vô hiệu hóa ghép nối (chỉ áp dụng cho các thiết bị iOS đã jailbreak): Các thiết bị iOS đã jailbreak cho phép người dùng kiểm soát hành vi ghép nối của thiết bị.

Sử dụng loại adapter chỉ sạc: Đây là biện pháp cuối cùng mà bạn có thể sử dụng, rất hiệu quả nhưng bất tiện đôi chút. Bạn có thể mua loại adapter chỉ sạc, chúng có giá khá rẻ. Hoàn toàn không có vấn đề gì với loại adapter này. Chúng này giống như một chiếc dongle nhỏ mà bạn sẽ cắm vào cổng USB trước khi kết nối cáp sạc của điện thoại vào. Các chân kết nối đóng vai trò truyền dữ liệu sẽ được ngắt kết nối trong dongle này, để chỉ cho phép điện được truyền tải điện qua kết nối mà thôi.

Tuy nhiên loại adapter này cũng có một nhược điểm nho nhỏ, đó là chúng chỉ hỗ trợ sạc với nguồn điện giới hạn ở mức 1A, đồng nghĩa với việc bạn không thể sử dụng bất kỳ công nghệ sạc nhanh nào khác. 1A là công suất tối đa mà bạn nhận được. Tuy nhiên, nhiều cổng sạc USB công cộng thậm chí còn có tốc độ sạc chậm hơn. Ngoài ra, có một điều đáng chú ý là các thiết bị sẽ chỉ được sạc ở 500mA (0.5A) từ cổng USB của máy tính, vì vậy, chiếc adapter này có thể tăng tốc độ sạc nếu bạn đang sạc thiết bị từ máy tính xách tay hoặc máy tính để bàn.

Nếu bạn đang sử dụng các thiết bị Android, bạn cũng có thể mua các loại cáp chỉ sạc hoạt động giống như một dongle, khi đó các chân truyền dữ liệu trong cáp sẽ bị thiếu, dẫn đến việc các kết nối nhằm mục đích trao đổi dữ liệu sẽ không bao giờ thực hiện được qua cáp. Còn đối với các thiết bị sử dụng cổng Lightning của Apple, có vẻ như hiện nay vẫn chưa có các sản phẩm cáp Lightning-to-USB chỉ sạc nào trên thị trường. Tuy nhiên, người dùng iOS vẫn có thể sử dụng các các adapter chỉ sạc, chúng có thể hoạt động được với cả iPhone và điện thoại Android.

Cuối cùng, cách bảo vệ tốt nhất giúp chống lại các hành vi xâm phạm nằm ở chính nhận thức của bạn. Hãy luôn giữ cho thiết bị của bạn luôn được sạc đủ năng lượng cần thiết, thường xuyên cập nhật các tính năng bảo mật được cung cấp bởi hệ điều hành (mặc dù chúng không dễ sử dụng và mọi hệ thống bảo mật đều có thể bị khai thác) và cuối cùng, tránh cắm điện thoại vào các trạm sạc và máy tính không xác định giống như cách bạn tránh không mở các file đính kèm trong mail từ người gửi không xác định vậy.